

AT-NO: JP02004164347A

DOCUMENT-IDENTIFIER: JP 2004164347 A

TITLE: IC CARD AND METHOD FOR PRINCIPAL AUTHENTICATION USING  
THE SAME

PUBN-DATE: June 10, 2004

INVENTOR-INFORMATION:

NAME

SUZUKI, NAOHISA

COUNTRY

N/A

ASSIGNEE-INFORMATION:

NAME

DAINIPPON PRINTING CO LTD

COUNTRY

N/A

APPL-NO: JP2002330155

APPL-DATE: November 14, 2002

INT-CL (IPC): G06K019/10, G06F015/00 , G06K019/07

ABSTRACT:

PROBLEM TO BE SOLVED: To provide an IC card that has a display part, an input part, a biometric information detection part and a transmission part, and a method for principal authentication using it.

SOLUTION: The IC card has on a surface at least the display part, an operation part and the biometric information detection part, and integrates in the interior at least an information storage part for storing reference biometric information, a biometric information collation part, a control part, a power supply part and a communication part. A user of the card is authenticated as the principal at least through a power application step of power application from the operation part, a biometric information input request command input step, a biometric information input permission message display step of displaying a biometric information input permission message on the display part, a biometric information detection step of detecting biometric information in the biometric information detection part, a biometric information collation step of collating the input biometric information with the reference biometric information, and a collation result display step of displaying a matching result of collation on the display part.

COPYRIGHT: (C) 2004, JPO

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-164347

(P2004-164347A)

(43) 公開日 平成16年6月10日(2004.6.10)

(51) Int.Cl. <sup>7</sup>	F I	テーマコード (参考)
G06K 19/10	G06K 19/00 S	5B035
G06F 15/00	G06F 15/00 330F	5B085
G06K 19/07	G06K 19/00 J	

審査請求 未請求 請求項の数 5 O L (全 8 頁)

(21) 出願番号	特願2002-330155 (P2002-330155)	(71) 出願人	000002897
(22) 出願日	平成14年11月14日 (2002.11.14)		大日本印刷株式会社
		(74) 代理人	100111659
			弁理士 金山 聡
		(72) 発明者	鈴木 直久
			東京都新宿区市谷加賀町一丁目1番1号
			大日本印刷株式会社内
		Fターム(参考)	5B035 AA14 BB09 BC01 CA05 CA06
			CA12 CA23
			5B085 AE12 AE25 AE26

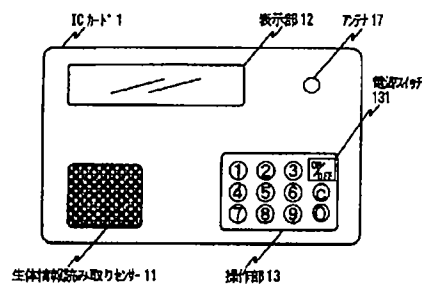
(54) 【発明の名称】 ICカード及びこれを使用する本人の認証方法

## (57) 【要約】

【課題】表示部と、入力部と、生体情報検出部と、送信部を有するICカード及びこれを使用する本人の認証方法を提供する。

【解決手段】表面に少なくとも表示部と、操作部と、生体情報検出部とを形成し、内部には少なくとも参照用生体情報を格納する情報格納部と、生体情報照合部と、制御部と、電力供給部と、通信部とを内蔵したICカードと、少なくとも、操作部によって電源を入力する電源入力ステップと生体情報入力要請コマンド入力ステップと、表示部に生体情報入力許可メッセージを表示する生体情報入力許可メッセージ表示ステップと、生体情報検出部によって生体情報を検出する生体情報検出ステップと、入力された生体情報と参照用生体情報を照合する生体情報照合ステップと、照合一致の結果を表示部に表示する照合結果表示ステップによって、該カードの使用者が本人であることを認証する

【選択図】 図1



## 【特許請求の範囲】

## 【請求項 1】

表面に少なくとも表示部と、操作部と、生体情報検出部とを形成し、内部には少なくとも参照用生体情報を格納する情報格納部と、生体情報照合部と、制御部と、電力供給部と、通信部とを内蔵したことを特徴とする IC カード。

## 【請求項 2】

前記操作部には、少なくとも 10 キーと電源オン、オフのための電源入力キーを設けたことを特徴とする請求項 1 に記載の IC カード。

## 【請求項 3】

前記生体情報検出部は、指紋を検出するセンサーであることを特徴とする請求項 1 ～ 2 何れか 1 項に記載の IC カード。 10

## 【請求項 4】

請求項 1 ～ 3 何れか 1 項に記載の IC カードを使用し、少なくとも、操作部の電源入力キーによって電源を入力する電源入力ステップと、操作部の 10 キーによって生体情報入力要請コマンドを入力する生体情報入力要請コマンド入力ステップと、表示部に生体情報入力許可メッセージを表示する生体情報入力許可メッセージ表示ステップと、生体情報検出部によって生体情報を検出する生体情報検出ステップと、入力された生体情報と参照用生体情報を照合する生体情報照合ステップと、照合一致の結果を表示部に表示する照合結果表示ステップによって、該 IC カードの使用者が本人であることを認証することを特徴とする IC カードを使用する本人の認証方法。 20

## 【請求項 5】

前記生体情報入力要請コマンドは、入力する本人のみが知る秘密番号であることを特徴とする請求項 4 に記載の IC カードを使用する本人の認証方法。

## 【発明の詳細な説明】

## 【0001】

## 【発明の属する技術分野】

本発明は、本人認証のための IC カード及び、認証方法に関し、詳しくは IC カードなどの表面に入力のためのキー、手順などを表示する表示部、指紋検出センサーを設け、指紋が一致して初めて目的とするステップに移行できるようにした IC カードとそれを使用する本人の認証方法に関する。 30

## 【0002】

## 【従来の技術】

近年、パーソナルコンピュータや携帯電話を利用する電子商取引が急速に普及しつつある。

インターネット等を利用した電子商取引において、本人を確認する手段の多くは入力されたパスワードを登録されたパスワードと照合することによって行われている。

ところが、パスワードは解読されやすい番号としていることが多いために盗まれたり、解読されて悪用される事件が多発している。

## 【0003】

そのため、カード等を利用した電子商取引等においては、偽造、盗用されたカードが使用されるケースも増加しており、当面はカードのパスワードを盗用、漏洩から確実に護ることが先決である。 40

## 【0004】

そこで、上記課題解決の為の技術がいくつか開示されている。

たとえば、指紋読み取り装置と、指紋情報判定器と、端末使用許可情報記録器と、指紋情報を登録するメモリと、無線の送受信器と、不正利用されたときの報知手段であるスピーカーなどを備えた認証カードが開示されている（特許文献 1 参照）。

上記認証カードは不正利用された場合、スピーカーで知らせたり、無線装置によって外部端末に警報を送信することができるが認証カード自らがカードに対する不正利用防止手段を実行していない。また、可変データの表示部を有しないために手順の表示や、取引情報 50

の表示を行うことができない。

【0005】

また、指紋検出手段と、指紋記憶手段と、指紋照合手段からなる指紋認証装置と、無線発信装置を搭載した携帯機器／端末で、認証終了後、該無線発信装置からアクセス許可信号を受信装置に送信し、販売製品、または提供役務に対するアクセス権を確保する装置及び方法が開示されている（特許文献2参照）。

この発明の携帯機器／端末にはデータ入力部についての記載が無いために、本人認証された場合にアクセス権確保の信号を送信するだけで、携帯機器／端末単独でのデータ入力及び表示が行われない。特許文献2に記載の請求項10、11で、携帯機器／端末は、携帯電話、またはPHSであるとしてデータの入力を可能としているが、この場合電話会社との契約が必要であり、利便性を損なうという欠点がある。

10

【0006】

【特許文献1】

特開平11-134302号公報

【特許文献2】

特開2002-82914号公報

【0007】

【発明が解決しようとする課題】

そこで本発明は、携帯電話等の携帯機器に代る表示部と、入力部と、生体情報検出部と、送信部を有するICカード及びこれを使用する本人の認証方法を提供する。

20

【0008】

【課題を解決するための手段】

前記課題の目的を達成するために本発明のICカードの請求項1に記載の発明は、表面に少なくとも表示部と、操作部と、生体情報検出部とを形成し、内部には少なくとも参照用生体情報を格納する情報格納部と、生体情報照合部と、制御部と、電力供給部と、通信部とを内蔵したことを特徴とするものである。

【0009】

また、請求項2に記載の発明は、請求項1に記載の発明において、操作部には、少なくとも10キーと電源オン、オフのための電源入力キーを設けたことを特徴とするものである。

30

【0010】

また、請求項3に記載の発明は、請求項1～2何れか1項に記載の発明において、生体情報検出部は、指紋を検出するセンサーであることを特徴とするものである。

【0011】

また、請求項4に記載の発明のICカードを使った本人認証方法は、請求項1～3何れか1項に記載のICカードを使用し、少なくとも、操作部の電源入力キーによって電源を入力する電源入力ステップと、操作部の10キーによって生体情報入力要請コマンドを入力する生体情報入力要請コマンド入力ステップと、表示部に生体情報入力許可メッセージを表示する生体情報入力許可メッセージ表示ステップと、生体情報検出部によって生体情報を検出する生体情報検出ステップと、入力された生体情報と参照用生体情報を照合する生体情報照合ステップと、照合一致の結果を表示部に表示する照合結果表示ステップによって、該カードの利用者が本人であることを認証することを特徴とするものである。

40

【0012】

また、請求項5に記載の発明は、請求項4に記載の発明において、生体情報入力要請コマンドは、入力する本人のみが知る秘密番号であることを特徴とするものである。

【0013】

【発明の実施の形態】

以下図面を参照して、本発明のICカード及びこれを使用する本人の認証方法の好適な実施形態について説明する。

また、本実施の形態の説明では生体情報検出手段として指紋検出手段の例で説明する。

50

## 【0014】

図1は、本発明のICカードの一実施形態の概略正面図、図2は、図1に示すICカードの内部構成を概略的に示すブロック図、図3は、指紋検出センサーの一実施形態の概略正面図、図4は、本発明のICカードを使用する本人の認証方法の認証フロー図、図5は、本発明のICカードの一実施形態の概略正面図、である。

## 【0015】

図1において、本発明のICカード1の正面には、生体情報読み取りセンサー（以下指紋センサーという。）11、表示部12、操作部13が設けられている。

ICカードの中には接触型ICカードがあり、カードの表面に形成された外部端末接続端子（外部端子）と外部端末を接続させてICカードに格納されている情報を読み取り、外部端末から送信される情報を読み書きするようになっているが、本実施の形態では、非接触型ICカードでアンテナ17によって情報の受信、送信を行う。

したがって、本図では図示しないが、接触型ICカードの場合は、ICカード1の表面に外部端子が設けられている。

上記の部品以外に、図示していないが、ICカードの表面には固定情報としてICカードの名称、デザインなどが印刷されている。

また、ICカード所持者の識別情報として、ICカード所持者の顔画像、IDコードが、ICカード利用のための情報として、ICカードの利用有効期間または有効期限等が印字、または打刻されている。

## 【0016】

図1の操作部は、ICカードの所持者が操作部13を右手の指で操作できるように右側に配置されている。その時に左手の指は、ICカードを支え、指紋センサー11に自然に触れるように配置されている。

操作部のボタンは、図1では0～9までの数字ボタンと、クリアボタンが形成されているが、数字ボタンにアルファベットや、仮名などの機能を持たせることもできる。また、図1では、親指で操作しやすいように、数字を縦横に並べて配置しているが、例えば、図5に示すように横長に並べても良い。

指紋センサー11については、図3で詳細に説明する。

また、表示部12には、公知の液晶や、電気泳動等の表示材料が使用される。

これらの部品は、図示している大きさに拘るものではなく、ICカードのデザインや、機能に応じて各部品の大きさ、配置位置が決定される。

## 【0017】

図1を参照して、ICカードによる本人認証の方法について説明する。

まず、左手と右手でICカード1を支え、右手の親指、または人差指で操作部13の電源ボタン131を押す。

電源がオンになると表示部12にはパスワード、または指紋入力要請コマンドの入力を要請するメッセージが表示される。

ICカードの所持者は、10キーによってパスワード、または指紋入力要請コマンドを入力する。

ICカードは、入力されたパスワード、または指紋入力要請コマンドと参照用に格納されているパスワード、または指紋入力要請コマンドと照合して、一致している事が確認されるとICカードは、表示部に指紋検出許可メッセージを表示する。

## 【0018】

ICカード所持者は、指紋センサーに登録している指を押し当てて、指紋を検出する。

指紋センサーは、採取した指紋データと、ICカードに格納されている参照用指紋情報を照合する。

照合の結果一致していれば、照合一致の結果を表示部に表示する。

不一致の場合、ICカードは、理由を表示して、再度指紋を検出するよう表示部12にメッセージを送る。エラー回数が定められた回数以上になった場合は、カードを一旦ロックし、ICカード発行機関にICカードを持参するようメッセージを表示する。

## 【0019】

従来のICカードは、端末と交信して、最初のステップでパスワードを入力し、一致していれば、直ちに取引が許可されていたが、本発明のICカードの場合は、更にその先に指紋照合のチェックを行うために、パスワードが盗用され、実行されても次の関門として指紋照合を行う必要があり、悪用を困難にしている。

このように、指紋センサーとの併用で2重のチェックを実行するためには、少なくともパスワードなどを入力するための操作部の入力キー、適切なメッセージを表示するための表示部が必要であることが判る。

## 【0020】

指紋照合の結果、ICカードの所持者が本人であることが証明されると、表示部12には、例えば銀行取引や、電子商取引などのアプリケーションコード（コマンド）を操作部13から入力するよう、指示メッセージが表示される。

ICカード所持者がICカードの操作部からアプリケーションコマンドを入力すると、ICカードの発信部のアンテナ17からはアプリケーション端末に対しアクセス信号が送信される。

## 【0021】

図2を参照してICカードの内部構成について説明する。

本発明のICカード1は、薄い金属またはプラスチックの外装部材に一体的に取りつけられた指紋センサー11、表示部12、操作部13と、内部に組み込まれた電源14、制御部材15、16、無線インターフェース部材17、18、情報格納部（メモリ）19で構成されている。

ICカード本体は、前述のようにプラスチックの成形によっても金属プレートの組み立てによっても何れでも良い。

但し、カードを外部端末に挿入して、または、カード本体を駆動させてデータ処理を行う場合は、カードの外形が国際標準を満足していることが必要である。

また、カードの外装材が金属の場合は、アンテナ周辺部に対し信号の送受信を妨げないような配慮が必要である。

## 【0022】

電源ボタン131によって電源14がオンになると、制御部1（15）、制御部2（16）等の制御部に電力が供給される。制御部1（15）は、通信制御部を制御し、所定の情報を送受信する。制御部2（16）は、表示部に表示電力を供給し、更に指紋センサー内の制御部に対して必要な電力を供給する。

制御部1（15）と、制御部2（16）は一体化することもできる。

また、図示していないが前記それぞれの制御部、または、何れかの制御部は、RAM、ROMを備えることができる。

無線インターフェース部材は、アンテナ17と、コントローラ18で図示されているが、1チップ型ブルートゥース集積回路のように一体化されたものや、赤外線タイプの送受信部材であっても良い。

情報格納部（メモリ）19には、表示部に表示する記号や文字のパターンデータや、駆動、表示プログラム、操作部から入力されたコマンド情報を一時保管するプログラムを格納することができる。

また、登録された参照用指紋データや、参照用パスワードや、アプリケーション毎の保管データをファイル別に格納することができる。

## 【0023】

指紋センサー11には、指紋の特徴を認識して、その組み合わせで指紋パターンを生成する指紋メモリ、認識回路が組み込まれている。指紋が指紋センサーによって検出された時に指紋の特徴をデータにして制御部2（16）を介して情報格納部（メモリ）19に登録する。

## 【0024】

図3を参照して指紋センサー11の一実施形態について説明する。

指紋センサー１１は、指が接触する表面がマトリックス状に細分化された複数の画素ユニットで構成され、それぞれの画素ユニットにセンサー回路を有する凹凸センサー部、指紋メモリ、認識回路が接続されている。

凹凸センサー部に配置されたセンサー素子は、層間絶縁膜上に配置された接触面を有する接触電極と接触電極に接続された配線層で構成される。

接触電極は、画素ユニットの最表面に配置され、指が接触することによって、発生する静電容量を検知する。

接触電極で検知された信号は、配線層で認識回路に伝搬される。

このセンサー素子では、接触電極の静電容量を測定し接触面が触れている部分の指紋の凹凸を検知する。

上述の静電容量方式のほかに光学方式の指紋検出方法がある

【００２５】

図４を参照して本発明のＩＣカードを使用する本人の認証方法の認証手順について説明する。

まず、ステップ１（以下Ｓ１という）で、ＩＣカードの表面に形成された電源ボタンを押す。ＩＣカードの所定の部品に電力が供給され表示部にパスワード、または指紋入力要請コマンドの入力を要請するメッセージが表示される。

ＩＣカード所持者は、操作部の１０キーによってパスワード、または指紋入力要請コマンドを入力する（Ｓ２）。ＩＣカードは入力されたパスワード、または指紋入力要請コマンドと、参照用に格納されているパスワード、または指紋入力要請コマンドと照合して、一

【００２６】

ＩＣカード所持者は、指紋センサーに登録している指を押し当てて、指紋を検出する。登録する指は親指でも人差指でも、複数の指でもよい。

登録している指を指紋センサーに押し当てて指紋を検出する（Ｓ３）。指紋センサーは、検出した指紋情報とＩＣカードのメモリ部に格納されている登録指の参照用指紋情報とを照合する（Ｓ４）。

照合の結果一致していれば、照合一致の結果を表示部に表示する。

不一致の場合、ＩＣカードは、再度指紋を検出するよう表示部１２にメッセージを送る（Ｓ８）。エラー回数が定められた回数以上になった場合は、カードを一旦ロック（Ｓ９）し、ＩＣカード発行機関にＩＣカードを持参するようメッセージを表示する。

【００２７】

指紋照合の結果、該ＩＣカードの所持者が本人であることが証明されたら、表示部は、例えば銀行取引や、電子商取引などのアプリケーションコード（コマンド）を操作部１３から入力するようメッセージを表示する。

ＩＣカード所持者は、希望するアプリケーションコマンドを入力する（Ｓ５）。

ＩＣカードのアンテナからはアプリケーション端末に対しアクセス信号を送信し交信する（Ｓ６）。

交信した結果を表示部に表示する（Ｓ７）。

【００２８】

【発明の効果】

１）請求項１から３に記載のように、表面に少なくとも表示部と、１０キーと電源入力キーからなる操作部と、指紋センサーなどの生体情報検出部を形成し、内部には少なくとも参照用生体情報を格納する情報格納部と、生体情報照合部と、制御部と、電力供給部と、通信部を内蔵したことによってＩＣカードを立ち上げる際のセキュリティを高めることができ、ＩＣカードの所持者以外の悪用を防ぐことができる。

２）請求項４、５に記載のように、請求項１～３何れか１項に記載のＩＣカードを使用し、少なくとも、操作部の電源入力キーによって電源を入力する電源入力ステップと、操作部の１０キーによってパスワードなど本人のみが知る秘密コマンドを入力する生体情報入力要請コマンド入力ステップと、表示部に生体情報入力許可メッセージを表示する生体情

10

20

30

40

50

報入力許可メッセージ表示ステップと、生体情報検出部によって生体情報を検出する生体情報検出ステップと、入力された生体情報と参照用生体情報を照合する生体情報照合ステップと、照合一致の結果を表示部に表示する照合結果表示ステップによって、該カードの使用者が本人であることを認証することによってＩＣカード使用する前に２重のチェックをかけることができる。

【図面の簡単な説明】

【図１】本発明のＩＣカードの一実施形態の概略正面図

【図２】図１に示すＩＣカードの内部構成を概略的に示すブロック図

【図３】指紋検出センサーの一実施形態の概略正面図

【図４】本発明のＩＣカードを使用する本人の認証方法の認証フロー図

10

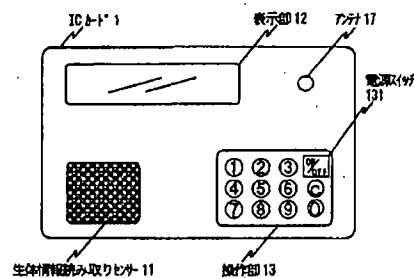
【図５】本発明のＩＣカードの一実施形態の概略正面図、

【符号の説明】

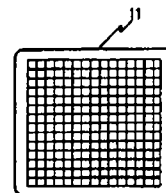
- １， １ｂ    ＩＣカード
- １１， １１ｂ    生体情報読み取りセンサー
- １２， １２ｂ    表示部
- １３， １３ｂ    操作部
- １４        電源
- １５        制御部１
- １６        制御部２
- １７， １７ｂ    無線インターフェースのアンテナ
- １８        無線インターフェースの通信制御部
- １９        情報格納部（メモリ）
- １３１， １３１ｂ    電源スイッチ

20

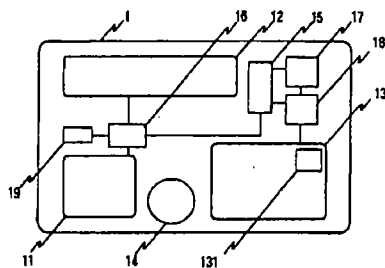
【図１】



【図３】

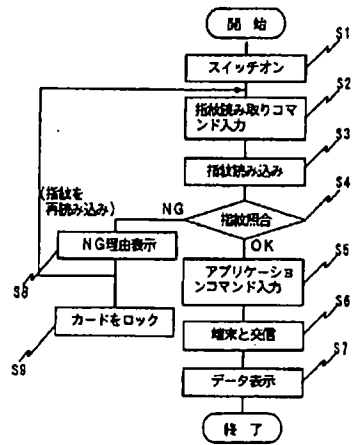


【図２】





【図 4】



【図 5】

